Sean Bruce

ISIT 328 Winter 2020

HW\_03

**CWE-ID**: CVE-2019-17180

**Description**: Valve Steam Client before 2019-09-12 allows placing or appending partially controlled filesystem content, as demonstrated by file modifications on Windows in the context of NT AUTHORITY\SYSTEM. This could lead to denial of service, elevation of privilege, or unspecified other impact.

**Vulnerability**: The Steam Client installs a "Steam Client Service" that runs as SYSTEM to update the steam application. This service executes from C:\Program Files (x86)\Common\Steam where permissions are properly set to only allow modification from SYSTEM or the Administrators group.

If the service encounters an error, it writes to the log file C:\Program Files (x86)\Steam\logs\service\_log.txt. This is a problem because this particular folder, and the parent folder, have permissions set to "Full Control" to any unprivileged user. A regular user can also trigger an error when the service starts by modifying or deleting the "C:\Program Files(x86)\Steam\bin\steamservice.dll" file that an unprivileged user also has "Full Control" of.

It also just so happens that the permissions for the "Steam Client Service" allow for starting and stopping by unprivileged users, which facilitates for easy triggering of the exploit.

To exploit this vulnerability, an unprivileged user can create a symlink between the "C:\Program Files (x86)\Steam\logs\service\_log.txt" file and any destination file that SYSTEM can write to. Next they would modify, move, or delete the "C:\Program Files (x86)\Steam\bin\steamservice.dll" to trigger an error message to be written. Finally they would start the "Steam Client Service" service to force the file write. The following video demonstrates writing to C:\Windows\System32\evil.dll and also C:\Windows\System32\drivers\pci.sys

to break the box.

**How**: A person can gain “Full Control” during a Steam client update. The client can gain the ability to start and stop Steam updates even though they are an unprivileged user. While the article does not elaborate on this, it mentions that from this state triggering further exploits would be easy.

The way the exploit is done is by triggering an error during the update process. To create the error, the hacker needs to modify or delete a specific Steam library before the update. The hacker also needs to create a symbolic link from an unprivileged account to a specific steam log file. Once the error is triggered, the unprivileged user can write to any file on the system with SYSTEM privileges.

**What can be lost**: Being that the unauthorized user can write to any file, it seems that the entire system is at risk. A hacker with malicious intent could destroy the whole system.